

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-49493

(43) 公開日 平成10年(1998) 2月20日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0		G 0 6 F 15/00	3 3 0 B
1/00	3 7 0		1/00	3 7 0 E
11/30	3 2 0		11/30	3 2 0 E
13/14	3 3 0		13/14	3 3 0 Z

審査請求 有 請求項の数 3 O L (全 5 頁)

(21) 出願番号 特願平8-206717

(22) 出願日 平成 8 年(1996) 8 月 6 日

(71) 出願人 000190541

新潟日本電気株式会社

新潟県柏崎市大字安田7546番地

(72) 発明者 樋口 敏明

新潟県柏崎市大字安田7546番地新潟日本電気株式会社内

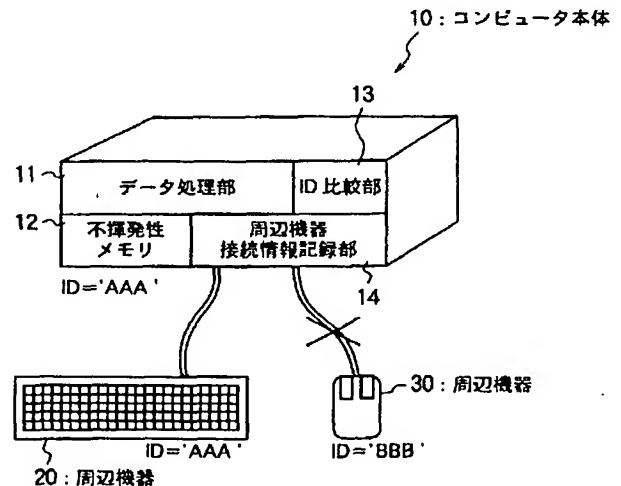
(74) 代理人 弁理士 稲垣 清

(54) 【発明の名称】 コンピュータシステム

(57) 【要約】

【課題】 コンピュータシステムの周辺機器の盗難を防ぐ。

【解決手段】 コンピュータ本体 10 及び周辺機器 20、30 に夫々識別番号を登録する不揮発性メモリを設け、コンピュータ本体 20 には、更に、コンピュータ本体の不揮発性メモリ 12 に登録された識別番号と周辺機器 20、30 の不揮発性メモリに登録された識別番号とを比較する識別番号比較部 13 と、識別番号比較部 13 の比較結果に基づいて周辺機器の使用を許可又は不許可とする周辺機器使用判定部 14 とを設ける。周辺機器は、登録された特定のコンピュータシステム以外では使用できなく、盗品の周辺機器の経済的価値は殆どなくなるので、周辺機器の盗難が抑止される。



## 【特許請求の範囲】

【請求項1】 コンピュータ本体と、該コンピュータ本体に接続される少なくとも1つの周辺機器とを備えるコンピュータシステムにおいて、コンピュータ本体及び周辺機器に夫々識別番号を登録する不揮発性メモリを設け、前記コンピュータ本体が、該コンピュータ本体の不揮発性メモリに登録された識別番号と周辺機器の不揮発性メモリに登録された識別番号とを比較する識別番号比較部と、該識別番号比較部の比較結果に基づいて周辺機器の使用を許可又は不許可とする周辺機器使用判定部とを備えることを特徴とするコンピュータシステム。

【請求項2】 前記周辺機器使用判定部は、前記周辺機器の不揮発性メモリに識別番号を登録する機能を更に有する、請求項1に記載のコンピュータシステム。

【請求項3】 前記識別番号比較部は、オペレータによって入力された識別番号と、前記コンピュータ本体の不揮発性メモリに登録された識別番号とを比較する機能を更に有する、請求項1又は2に記載のコンピュータシステム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、コンピュータシステムに関し、特にコンピュータシステムの周辺機器の盗難を抑止するためのセキュリティ技術に関する。

## 【0002】

【従来の技術】 コンピュータシステムのセキュリティとしては、コンピュータシステムに登録されたデータの保護と、コンピュータシステムを構成する装置の盗難防止の2つが重要である。コンピュータシステムにおけるデータのセキュリティに関しては、従来、内部データの保護を目的とする鍵による施錠や、パスワード照合による起動条件を付加する等により当事者以外の使用を排除する対策が知られている。しかし、コンピュータシステムの装置自体の盗難防止に関しては、殆ど対策が採られていない。

## 【0003】

【発明が解決しようとする課題】 周辺機器の盗難を防止する1つの方法として、周辺機器をある特定のコンピュータシステムにおいてのみ使用可能とすることが考えられる。しかし、周辺機器には、コンピュータシステム本体に備わっているようなデータ保護機能を設けることが一般的には出来ないので、このような対策を採ることは困難である。

【0004】 本発明は、上記に鑑み、コンピュータシステムの周辺機器の盗難を防止することが出来るコンピュータシステムを提供することを目的とする。

## 【0005】

【課題を解決するための手段】 本発明のコンピュータシステムは、コンピュータ本体と、該コンピュータ本体に

接続される少なくとも1つの周辺機器とを備えるコンピュータシステムにおいて、コンピュータ本体及び周辺機器に夫々識別番号を登録する不揮発性メモリを設け、前記コンピュータ本体が、該コンピュータ本体の不揮発性メモリに登録された識別番号と周辺機器の不揮発性メモリに登録された識別番号とを比較する識別番号比較部と、該識別番号比較部の比較結果に基づいて周辺機器の使用を許可又は不許可とする周辺機器使用判定部とを備えることを特徴とする。

10 【0006】 本発明のコンピュータシステムの好ましい態様では、上記周辺機器使用判定部が、周辺機器の不揮発性メモリに識別番号を登録する記録機能を更に有する。これにより、例えば、コンピュータ本体と全く同じ識別番号又は関連する識別番号を周辺機器に登録することが出来る。

20 【0007】 また、上記識別番号比較部が、オペレータによって入力された識別番号と、前記コンピュータ本体の不揮発性メモリに登録された識別番号とを比較する機能を更に有することも好ましい態様である。この場合、コンピュータ本体のセキュリティも向上する。

30 【0008】 本発明のコンピュータシステムでは、周辺機器の使用に先立って、コンピュータ本体の不揮発性メモリに登録された識別番号と周辺機器の不揮発性メモリに登録された識別番号とを識別番号比較部で比較し、その比較結果に基づいて周辺機器使用判定部において周辺機器の使用を許可し又は不許可とするため、事前に登録された周辺機器のみが使用可能となる。かかるコンピュータシステムが設備されるコンピュータシステムの大半を占めるようになれば、盗品の周辺機器の使用は排除される。

## 【0009】

【発明の実施の形態】 本発明の実施形態例に基づいて本発明を更に詳細に説明する。図1は、本発明の一実施形態例のコンピュータシステムを示す模式的ブロック図である。コンピュータシステムは、コンピュータ本体10と、複数の(図面上で2つの)周辺機器20、30とから構成される。コンピュータ本体10は、通常の日データ処理を行うデータ処理部11と、コンピュータ本体の識別番号(ID)を登録するための不揮発性メモリ12と、コンピュータ本体10のIDと周辺機器20、30のIDとを比較するID比較部13と、ID比較部13の比較結果に従って周辺機器の使用の許可又は不許可を判定する機能を有する周辺機器接続情報記録部14とを有する。双方の周辺機器20、30には、夫々、IDを登録するための不揮発性メモリが設けられている。コンピュータ本体及び周辺機器の不揮発性メモリには、例えばフラッシュROMが使用できる。

50 【0010】 図1に示したように、コンピュータ本体10の不揮発性メモリ12には、コンピュータ本体の識別記号、"AAA"が記録されている。双方の周辺機器2

## 3

0、30にも夫々その識別記号(ID)が不揮発性メモリに登録されており、入力装置を成す一方の周辺機器20には識別記号"AAA"が、マウスとして構成される他方の周辺機器30には識別記号"BBB"が夫々記録されている。ここで、コンピュータ本体10の識別記号"AAA"と、マウス30の識別記号"BBB"とが異なるので、マウス30は、コンピュータ本体10のID比較部13からの情報に基づいて、周辺機器接続情報記録部14によって本コンピュータシステムから排除される。

【0011】図2は、上記実施形態例のコンピュータシステムにおける処理を示すフロー図である。コンピュータシステムが起動されると(ステップS1)、コンピュータ本体のIDが登録されているか否かがチェックされる(ステップS2)。コンピュータ本体のIDが不揮発性メモリ内に登録されていないければ、ID登録のキー入力力が前後2回促され、この2回入力されたIDが相互に同じであることが確認される(ステップS3、S4)。確認されたIDをコンピュータ本体のIDとしてコンピュータ本体の不揮発性メモリに登録した後に(ステップS5)、ステップS8に進んでコンピュータ本体の不揮発性メモリをマスクする。このマスクにより、再び電源が投入されるまでは少なくともIDのリード/ライトを禁止する。

【0012】ステップS2でコンピュータ本体のIDの登録済が確認されると、オペレータに対してID照合のためのキー入力力が促される。IDのキー入力があると(ステップS6)、コンピュータ本体の不揮発性メモリに登録されたIDと、キー入力されたIDとが照合される(ステップS7)。照合の結果、双方のIDが不一致であると、ステップS6に戻り再度のID入力力が促される。双方のIDが一致すれば、ステップS8の不揮発性メモリのマスクに移る。

【0013】ステップS8に引き続き、周辺機器の接続の有無がチェックされ(ステップS9)、接続が確認された周辺機器の1つについて、そのIDが登録されているか否かがチェックされる(ステップS10)。IDが未登録であれば、周辺機器接続情報記録部は、周辺機器の不揮発性メモリに、コンピュータ本体のIDと同じIDを登録する(ステップS11)。その後、通常の処理に従って周辺機器の使用に必要なセットアップを行い(ステップS12)、周辺機器接続情報記録部に当該周辺機器の接続許可を登録し(ステップS13)、ステップS18に移る。

【0014】ステップS10で、周辺機器のIDが既に登録されていれば、そのIDがコンピュータ本体のIDと同じであるか否かがチェックされる(ステップS14)。周辺機器のIDとコンピュータ本体のIDとが一致しなければ、その周辺機器の使用を不許可にし(ステップS15)、周辺機器接続情報記録部に当該周辺機器

## 4

の接続が不許可である旨を登録し(ステップS16)、次いで、ステップS18に移る。

【0015】ステップS14で双方のIDが一致すれば、周辺機器接続情報記録部に、当該周辺機器の接続許可の旨を登録し(ステップS17)、その周辺機器の不揮発性メモリをマスクすることにより(ステップS18)、少なくとも再度電源が投入されるまではその後のリード及びライトを禁止し、当該周辺機器の処理を終了する。その他に周辺機器があれば(ステップS19)、ステップS9に戻り、その周辺機器について前述の処理と同様の処理が行われ、その他に周辺機器がなければ、周辺機器についての処理を全て終了する。その後、コンピュータシステムはブート処理に移る(ステップS20)。

【0016】上記実施形態例では、本コンピュータシステムで利用できる周辺機器20(図1)、及び、使用できない周辺機器30についての情報は、コンピュータ本体10内部の周辺機器接続情報記録部14に登録してあるので、いつでも参照可能である。

【0017】なお、上記実施形態例では、不揮発性メモリのマスキにより、再度電源が投入される迄のリード及びライトを禁止した例を示したが、これに代えて、不揮発性メモリにおけるIDの登録後は、いかなる書換えをも禁止することも出来る。この場合、セキュリティは更に向上する。

【0018】また、周辺機器接続情報記録部によって、周辺機器の使用の許可又は不許可を判定する例を挙げたが、これに代えて、周辺機器使用判定部を別のプログラムとして設けてもよい。また、照合のためにコンピュータ本体のIDをキー入力して、これと登録されたIDとを照合する例を挙げたが、これに加えて、オペレータ自身のIDを入力して照合するようにしてもよい。

【0019】以上、本発明をその好適な実施形態例に基づいて説明したが、本発明は、上記実施形態例の構成にのみ限定されるものではなく、上記実施形態例の構成から種々の修正及び変更を施したコンピュータシステムも、本発明の範囲に含まれる。

## 【0020】

【発明の効果】以上、説明したように、本発明のコンピュータシステムによると、コンピュータ本体及び周辺機器の双方のIDを比較照合した結果に基づいて周辺機器の使用を許可するように構成したので、コンピュータシステムの周辺機器の盗難を抑止する効果がある。

## 【図面の簡単な説明】

【図1】本発明の一実施形態例のコンピュータシステムの模式的ブロック図。

【図2】図1の実施形態例のコンピュータシステムにおける処理を示すフローチャート。

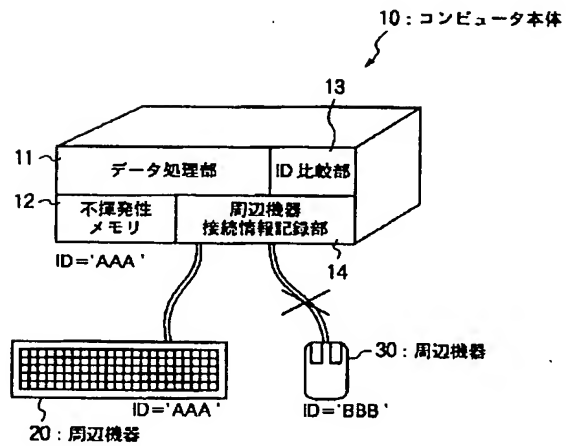
## 【符号の説明】

10 コンピュータ本体

- 11 データ処理部
- 12 不揮発性メモリ
- 13 周辺機器接続情報記録部

- 14 ID比較部
- 20 周辺機器 (入力装置)
- 30 周辺機器 (マウス)

【図1】



【図2】

